ABSTRACT

A method, system, computer program product, and method of doing business by providing a provable chain of evidence for data stream(s) created by one or more components (such as input/output devices and application processing components). Components that create the evidence collection are authenticated. A unique identifier of each such component is included within cryptographically-protected information that is added to the evidence collection. A digital signature is preferably used for the cryptographic protection, thereby digitally notarizing the evidence collection. The authenticity and integrity of the evidence collection can be verified. In preferred embodiments, the authenticated identities of components providing the evidence can also be determined from the cryptographically-protected information. One or more data streams may be included within the evidence collection to establish information such as the date and time the evidence collection was captured, the geographic location where the capture was performed, an identification of a person performing the evidence capture, and so forth. When present in a provable chain of evidence, these types of additional evidence are provided by authenticated components which are identified within the cryptographically-protected information.